



subjects. I have also spoken to confidential human sources, suspects, defendants, witnesses, and other experienced investigators concerning the methods and practices of the criminal element. I have gained experience through training at the FBI Academy and training provided by the Complex Financial Crimes Section within the FBI. This training pertained to interviewing and interrogation techniques, arrest procedures, search and seizure, search warrant applications, methods used by fraudsters and various other crimes and investigative techniques. I have had the opportunity to supervise, lead, observe and review numerous investigations, in order to gain an understanding of the methods used by white collar criminals. At all times during the investigation described herein, I have acted in my official capacity as Special Agent with the FBI.

2. Since the affidavit is being prepared for the limited purpose of a Verified Complaint *in Rem*, I have not included each and every fact known to me concerning this investigation. I only set forth the facts that I believe are necessary to support a reasonable belief that the government will be able to meet its burden of proof at trial.

3. The information contained in this affidavit is based on, among other things, my personal knowledge, and observations during the course of this investigation, information conveyed to me by the victims(s), the divisions of the FBI, the public, other government agencies, and officials, law enforcement personnel, both domestic and foreign, and my review of records, documents and other evidence obtained during this investigation.

**PROPERTY TO BE SEIZED**

4. This affidavit is submitted in support of a Verified Complaint *in Rem* for the following asset ("DEFENDANT PROPERTY"):

a) Approximately \$378,625.12 USDT In Cryptocurrencies Seized from Binance User ID 201812576.

a. (DEFENDANT PROPERTY).

5. As set forth below, I submit there is probable cause to believe that the DEFENDANT PROPERTY constitutes proceeds from violations of Wire Fraud, 18 U.S.C. § 1343 and property involved in a money laundering transaction or money laundering conspiracy, in violation of 18 U.S.C. § 1957, or are traceable to such property. The DEFENDANT PROPERTY is, therefore, subject to forfeiture to the United States.

### **FORFEITURE AUTHORITY**

6. The DEFENDANT PROPERTY is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C), on the grounds that the funds contained in the above-listed account constitute proceeds that are directly traceable to violations of specified unlawful activities, specifically, proceeds traceable to wire fraud, in violation of 18 U.S.C. § 1343. The DEFENDANT PROPERTY is further subject to forfeiture to the United States pursuant to 18 U.S.C. §§ 981(a)(1)(C) and 981(a)(1)(A), on the grounds that the funds contained in the above-listed account constates proceeds that are directly traceable to money laundering, in violation of 18 U.S.C. § 1957. For reason set forth below, probable cause exists for the forfeiture of the DEFENDANT PROPERTY.

### **BACKGROUND ON CRYPTOCURRENCY**

7. Based on my training, research, education, and experience, I am familiar with the following relevant terms and definitions:

a. Cryptocurrency, a type of virtual and/or digital currency, is a decentralized, peer-to peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies.

Examples of cryptocurrency are ether, bitcoin, and Litecoin, etc. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a “blockchain,” which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.<sup>1</sup> Cryptocurrency is not illegal in the United States.

b. Ether, “ETH”, is a type of cryptocurrency. Payments or transfers of value made with ether are recorded in the Ethereum blockchain and thus are not maintained by any single administrator or entity. As mentioned above, individuals can acquire ether through exchanges (i.e., online companies which allow individuals to purchase or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), Ether ATMs, or directly from other people. Individuals can also acquire cryptocurrencies by “mining.” An individual can “mine” ether by using his/her computing power to solve a complicated algorithm and verify and record payments on the blockchain. Individuals are rewarded for this task by receiving newly created units of a cryptocurrency. Individuals can send and receive cryptocurrencies online using many types of electronic devices, including laptop computers and smart phones. Even though the public

---

<sup>1</sup> Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers. If, however, an individual or entity is linked to a public address, it may be possible to determine what transactions were conducted by that individual or entity. Ethereum transactions are therefore sometimes described as “pseudonymous,” meaning that they are partially anonymous. And while it’s not completely anonymous, Ethereum allows users to transfer funds more anonymously than would be possible through traditional banking and credit systems.

c. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or “public key”) and the private address (or “private key.”) A public address is represented as a case-sensitive string of letters and numbers, 26–25 characters long. Each public address is controlled and/or accessed through the use of a unique corresponding private key - the cryptographic equivalent of a password or PIN - needed to access the address. Only the holder of an address’ private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

d. Although cryptocurrencies such as ether have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes such as money laundering and is an oft used means of payment for illegal goods and services. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement’s efforts to track purchases. As of February 27, 2022, one ether is worth

approximately \$2,597.67 USD, though the value of ether is generally much more volatile than that of fiat currencies.

e. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device (“hardware wallet”), downloaded on a PC or laptop (“desktop wallet”), with an Internet-based cloud storage provider (“online wallet”), as a mobile application on a smartphone or tablet (“mobile wallet”), printed public and private keys (“paper wallet”), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (e.g. Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR code<sup>2</sup> with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a “recovery seed” (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase) or an API Key, as further explained below. I also know that individuals possessing cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies become further secured in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

---

<sup>2</sup> A QR code is a matrix barcode that is a machine-readable optical label.

f. Ethereum “exchangers” and “exchanges” are individuals or companies that exchange ether for other currencies, including U.S. dollars. According to the Department of Treasury, Financial Crimes Enforcement Network (“FinCEN”) Guidance issued on March 18, 2013, virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money services businesses.<sup>3</sup> Such exchanges and exchangers are required to register with FinCEN and have proper state licenses (if required under applicable state law). From my training and experience, I know that registered money transmitters are required by law to follow Bank Secrecy Act anti-money laundering (“AML”) regulations, “Know Your Customer” (“KYC”) protocols, and other verification procedures similar to those employed by traditional financial institutions. For example, FinCEN-registered cryptocurrency exchangers often require customers who want to open or maintain accounts on their exchange to provide their name, address, phone number, and/or the full bank account and routing numbers that the customer links to his/her exchange account. As a result, there is significant market demand for illicit cryptocurrency-for-fiat currency exchangers, who not only lack AML or KYC protocols but often advertise their ability to offer customers stealth and anonymity. These illicit exchangers often exchange fiat currency for cryptocurrencies, such as by meeting customers in person or by shipping fiat currency through the mail. Due to the illicit nature of these transactions and their customers’ desire for anonymity, such exchangers are frequently able to charge a higher exchange fee, often as high as 9-10% (in contrast to registered and BSA-compliant exchangers, who may charge fees as low as 1-2%).

---

<sup>3</sup> See “Application of FinCEN’s Regulations to Person Administering, Exchanging, or Using Virtual Currencies,” *available at* <https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering>.

j. Some companies offer cryptocurrency wallet services which allow users to download a digital wallet application onto their smart phone or other digital device. A user typically accesses the wallet application by inputting a user-generated PIN code or password. Users can store, receive, and transfer cryptocurrencies via the application; however, many of these companies do not store or otherwise have access to their users' funds or the private keys that are necessary to access users' wallet applications. Rather, the private keys are stored on the device on which the wallet application is installed (or any digital or physical backup private key that the user creates). As a result, these companies generally cannot assist in seizing or otherwise restraining their users' cryptocurrency. Nevertheless, law enforcement could seize cryptocurrency from the user's wallet directly, such as by accessing the user's smart phone, accessing the wallet application, and transferring the cryptocurrency therein to a law enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for a wallet (see above), investigators may be able to use the recovery seed phrase to recover or reconstitute the wallet on a different digital device and subsequently transfer cryptocurrencies held within the new wallet to a law enforcement-controlled wallet.

k. Slippage refers to all situations in which a market participant receives a different trade execution price than intended. Slippage occurs when the bid/ask spread changes between the time a market order is requested and the time an exchange or other market-maker executes the order.



## **FRAUD INVESTIGATION BACKGROUND**

8. The FBI is engaged in an investigation of a fraudulent romance scheme associated with a fraudulent investment scheme against individuals using the name Victoria Leah, and Samantha Zaitseva who appear to use unsuspecting victims as facilitators of the schemes.

9. Beginning in March 2023, Danny Shelton (SHELTON), of Kingsport, Tennessee, entered into a romantic relationship on-line using an app known as Telegram with an individual known to him as Samantha Zaitseva (ZAITSEVA). ZAITSEVA informed SHELTON that she lived in California and lived with her uncle who ran a successful crypto investment business. ZAITSEVA was able to convince SHELTON to invest more than \$400,000 in cryptocurrency.

10. ZAITSEVA instructed SHELTON to make multiple wire transfers in the amounts of \$30,000, \$260,000 and \$120,000 for the purpose of investing in cryptocurrency. SHELTON was told the funds would then be exchanged into cryptocurrency and forward to a company known to SHELTON as Paribu. SHELTON believed Paribu was a cyber currency exchange used by ZAITSEVA's uncles' business. The first transfer used Coinbase to transfer the funds to Paribu, who confirmed receipt of the funds. SHELTON was instructed to send the second transfer of \$260,000 to Crypto.com and then it would be forward to Paribu. Unbeknownst to SHELTON, this transaction was flagged, and the funds were frozen and are being held by Binance. SHELTON was instructed to send a third transfer of \$120,000 to Crypto.com, which was rejected by Crypto.com on grounds of suspicious activity with the account the funds were being directed to. SHELTON informed ZAITSEVA that the funds were rejected, at which time ZAITSEVA instructed SHELTON to send the funds directly to Paribu via a wire transfer. SHELTON began the process to wire the funds using SHELTON's bank, Bank of Tennessee.

11. In July 2023, SHELTON was informed that the second transaction of \$260,000 was frozen and currently in the possession of Binance. SHELTON was informed by Crypto.com to contact law enforcement regarding this account and the funds on the grounds of suspected fraud. SHELTON contacted the affiant who confirmed with Binance that SHELTON's \$260,000 had been transferred to cryptocurrency and frozen based on possible fraudulent activity associated with Monacie Latras, User ID 201812576 (DEFENDANT PROPERTY).

12. Based on this new information SHELTON contacted Bank of Tennessee located in Kingsport, TN in effort to stop the fourth transaction, which was a wire transfer of \$120,000 going to Paribu. Bank of Tennessee, working with SHELTON and affiant, was able to recovery the \$120,000 by stopping the wire transfer using internal financial institution procedures.

13. Based on the foregoing information, I believe there is probable cause that SHELTON was a victim involved in an investment scam to facilitate wire fraud. There is also probable cause to believe the funds in Binance User ID account 201812576 belong to SHELTON, who is also a victim of an investment scam.

14. Beginning in March 2023, Edward Skwor (SKWOR), of Savage, Minnesota, entered into a romantic relationship on-line using an app known as Telegram with an individual known to him as Victoria Leah (LEAH) a.k.a. Natalie Victoria. LEAH informed SKWOR that she lived in California and worked with her uncle who ran a successful crypto investment business. LEAH was able to convince SKWOR to invest more than \$250,000 in cryptocurrency.

15. With instructions provided by LEAH, SKWOR initiated multiple wire transfers to Crypto.com via Metropolitan Bank located in New York. The funds were then transitioned into cryptocurrency and forwarded to Paribu. LEAH indicated that Paribu was a crypto exchange that LEAH and her uncle uses and has their account with.

16. During the next three months, LEAH and LEAH's accomplices instructed SKWOR to make trades and SKWOR was provided documentation showing SKWOR's investments growing in value. When SKWOR's account reached a value of \$750,000, SKWOR was instructed by LEAH to make a large withdraw. SKWOR decided to withdraw \$240,000 to be forward to SKWOR's personal bank account.

17. SKWOR followed the instructions provided by LEAH and attempted to withdraw \$240,000. SKWOR received an email from Paribu indicating SKWOR needed to pay taxes on the gains in the account. SKWOR initiated a wire transfer of \$133,000 on June 20, 2023, to Crypto.com which would be forwarded to Paribu to cover the taxes owed. Paribu sent a follow-up email indicating Paribu received the funds, but SKWOR now needed to pay a fee due to the high amount SKWOR wanted to withdraw. SKWOR then initiated a wire transfer to CRYPTO.COM in the amount of \$77,000 which was rejected due to suspicious activity associated with the account the funds were to be forward to.

18. SKWOR informed Paribu the funds were rejected. Paribu informed SKWOR there would be a late fee added and now SKWOR owed \$95,872. Paribu then provided instructions for SKWOR to wire the funds directly to Paribu via an international bank in Hong Kong, which SKWOR complied with and initiated the wire transfer.

19. Crypto.com informed SKWOR that his wire transfer of \$133,000 was frozen by Binance based on suspicion of fraud and referred SKWOR to law enforcement. SKWOR contacted affiant who has confirmed with Binance that the SKWOR funds were in fact frozen and were held in the Binance Wallet belonging to, or associated with, Monacie Latras, Binance User ID 201812576 based on suspected fraud activity.

20. The contents of the DEFENDANT PROPERTY were seized on July 8, 2024, subsequent to a Warrant to Seize Property Subject to Forfeiture dated August 24, 2023, and executed, August 25, 2023, from Binance Holdings Limited, located in Grand Cayman, Cayman Islands and are currently being held in a FBI controlled Wallet ending in C31B. Based on the foregoing information, I believe there is probable cause that the contents of the DEFENDANT PROPERTY are proceeds from wire fraud and/or involved in money laundering transactions.

21. Based upon the foregoing information, it appears that the DEFENDANT PROPERTY contains funds constituting or traceable to proceeds of violations of 18 U.S.C. § 1343. As a result, the DEFENDANT PROPERTY is subject to civil forfeiture by the United States, pursuant to 18 U.S.C. § 981(a)(1)(C). Moreover, the DEFENDANT PROPERTY is involved in violations of 18 U.S.C. § 1957. THE DEFENDANT PROPERTY is further subject to civil forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(C) and 981(a)(1)(A), on the grounds that the DEFENDANT PROPERTY contained in the above-listed account constitutes proceeds that are directly traceable to violations of 18 U.S.C. § 1957.

22. The events described herein occurred in, and are situated in, the Eastern District of Tennessee and elsewhere. Accordingly, pursuant to 1355(b)(A) of Title 28, “A forfeiture action or proceeding may be brought in the district court for the district in which any of the acts or omissions giving rise to the forfeiture occurred”.

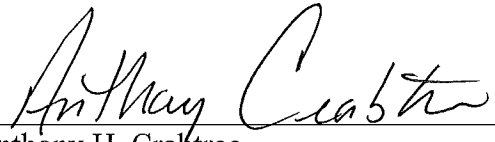
### **CONCLUSION**

23. The defendant property constitutes proceeds that are directly traceable to violations of 18 U.S.C. § 1343 (wire fraud) and is subject to civil forfeiture pursuant to 18

U.S.C. § 981(a)(1)(C) and constitutes property involved in or traceable to a transaction or attempted transaction in violation of 18 U.S.C. § 1957 (Money Laundering) and is subject to civil forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) and 981(a)(1)(C).

All of the above information is true and correct to the best of my knowledge.

FURTHER AFFIANT SAYETH NAUGHT.

  
\_\_\_\_\_  
Anthony H. Crabtree  
Special Agent  
Federal Bureau of Investigation

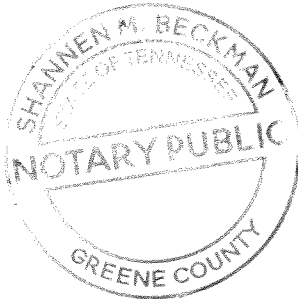
STATE OF TENNESSEE

COUNTY OF KNOX

On this 16<sup>th</sup> day of April, 2025, before me, personally appeared Anthony H. Crabtree in his capacity as a Special Agent with the Federal Bureau of Investigation, to me known to be the person described in and who executed the foregoing instrument, and acknowledged that she executed the same as his free act and deed.

IN WITNESS WHEREOF I have hereunto set my hand and Notarial Seal.

Subscribed to and sworn before me on this 16<sup>th</sup> day of April, 2025.



Shannen M. Beckman  
NOTARY PUBLIC

My Commission Expires: 3/24/2027